UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JASON COOPER and MEGHNA PARIKH, individually and on behalf of all others similarly situated, *Plaintiffs*, v. SLICE TECHNOLOGIES, INC., a Delaware corporation, and UNROLLME INC., a Delaware corporation, *Defendants*.	Case No. 1:17-cv-07102 The Honorable J. Paul Oetken Magistrate Judge Andrew J. Peck

PLAINTIFFS' RESPONSE TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

United States Supreme Court

United States Circuit Court of Appeals

United States District Court Cases

State Appellate Courts

Rules and Statutes

INTRODUCTION

Imagine a homeowner hires a cleaning company for a spring cleaning, entrusting that company with a key to his house. While cleaning the house, the cleaning company surreptitiously goes through the homeowner's cupboards and medicine cabinets recording all that it finds so that it can sell information about what breakfast cereals the homeowner eats to General Mills and what toiletries he uses to Proctor & Gamble. That is the analog equivalent to what is digitally happening in this case.

Plaintiffs Jason Cooper and Meghna Parikh, along with other consumers, downloaded a product called UnrollMe to clean up their email inboxes and help them unsubscribe from spam emails. Unbeknownst to Plaintiffs, however—and following an acquisition of UnrollMe by Slice Technologies, Inc., ("Slice") a data mining company—UnrollMe began collecting and selling Plaintiffs' emails to third parties. For example, UnrollMe sells emails between UnrollMe users and ride-sharing company Lyft to a competing ride-sharing company, Uber.

Based on Defendants' unauthorized collection and sale of their emails, Plaintiffs filed suit against UnrollMe Inc. and its data-mining parent company, Slice, which Defendants have now moved to dismiss for lack of Article III standing and for failure to state a claim. But Defendants' outrageous invasion of privacy is an actual, concrete injury establishing Article III standing, and Plaintiffs are entitled to relief under various federal and state laws. While Defendants make several different arguments, their basic defense is consent: you let us in so we can do

whatever we want. But that argument doesn't justify the cleaning service's conduct in the hypothetical above, and it doesn't work here. Defendants' motion to dismiss should be denied.

BACKGROUND

Defendants offer an "email management" service called UnrollMe to help users "clean up [their] inbox." (Compl. ¶¶ 2-3.)[1] Ostensibly, the "sole purpose" of UnrollMe is to "allow[] users to easily unsubscribe from mailing lists, newsletters and other unwanted emails." (*Id*. ¶ 2.) Specifically, UnrollMe purports to "rid [users'] email inboxes of junk by … mass unsubscrib[ing] from spam messages and … group[ing] categories of emails into a single email digest that would be sent to the user daily." (*Id*. ¶ 14.) Throughout the sign-up and installation process, users are implored to "[c]lean up your inbox," told that "[they're] just a few clicks away from a cleaner inbox," and informed that "[they're] all ready to go, time to clean your inbox & take a break from email spam." (*Id*. ¶¶ 20-25 & Figs. 1-6.) The initial sign-up screen notifies users that the service will allow them to "[i]nstantly see a list of all [their] subscription emails [and] [u]nsubscribe easily from whatever [they] don't want." (*Id*. ¶ 20 & Fig. 1.) Later screens inform users that "We found [a number of] subscriptions" and that "We'll let you know when we find new subscriptions." (*Id*. ¶¶ 24-25 & Figs. 5-6.) Finally, at the end of the process, users are told "All finished!," "That's it!," and "Okay, you're all set!" (*Id*.)

---

[1] "Compl." and "Complaint" refer to Plaintiffs' Consolidated Class Action Complaint, dkt. 29. On a motion to dismiss, this Court must accept all allegations in the complaint as true and draw all inferences in plaintiffs' favor. *City of New York v. Beretta U.S.A. Corp.*, 524 F.3d 384, 392 (2d Cir. 2008).

UnrollMe was originally launched in 2011, but was acquired in 2014 by data-mining company Slice. (*Id.* ¶¶ 14-15.) While the service is free, UnrollMe originally generated revenue by showing advertisements to users in their daily email digest. (*Id.* ¶¶ 14, 18.) After the acquisition by Slice, however, UnrollMe changed the way it makes money. (*Id.* ¶ 18.) What users don't know—and what they don't consent to—is that Defendants do more than just clean and organize users' email inboxes. Instead, Defendants scour the contents of users' emails for valuable data that they can—and do—sell to the highest bidder. (*Id.* ¶¶ 15-20, 27-28, 37, 40, 47.) For example, Defendants cull UnrollMe users' emails for e-commerce receipts, turning its users into an unwitting panel of online shoppers providing valuable market research that Defendants can sell. Defendants boast—to potential buyers of this data, not the UnrollMe users from whom they surreptitiously collect it—that they gather information from over 4.2 million online shoppers that can be turned into "actionable insights, furnishing brands and retailers with the answer to essential questions about digital commerce." (*Id.* ¶ 15.) To do so, Defendants use "technology that automatically identifies e-receipts within [email] inboxes, extract[ing] every available data point about every purchase at the item level," and that "measures all online purchases, using the same methodology, tied to the same consumer, including that consumer's historical purchase patterns to reveal loyalty and switching behavior." (*Id.* ¶¶ 16-17.) Again, Defendants then sell this information—collected from UnrollMe users without their knowledge or consent—to businesses seeking insight into consumer behavior. (*Id.* ¶ 17.) And Defendants sell not just

data gleaned from emails, but whole emails. (*See id.* ¶¶ 33-35, 37) (alleging that Defendants "sell[] collected emails to anyone willing to pay").

Upset that Defendants sold their emails to third parties—emails to which Defendants had only been granted access because they claimed to be simply decluttering UnrollMe users' inboxes—Plaintiffs Jason Cooper and Meghna Parikh filed this lawsuit alleging claims under the Wiretap Act, 18 U.S.C. § 2510 et seq., the Stored Communications Act, 18 U.S.C. § 2701 et seq., and various state law claims. Following a transfer from the Northern District of California to this Court, Defendants moved to dismiss Plaintiffs' Complaint.[2]

ARGUMENT

Defendants move to dismiss under Fed. R. Civ. P. 12(b)(1) for lack of Article III standing, and under Fed. R. Civ. P. 12(b)(6) for failure to state a claim.[3] Neither of these grounds supports dismissal. With respect to Article III standing, the invasion of Plaintiffs' privacy is a concrete injury in fact sufficient to establish standing.

---

[2] Pursuant to this Court's Individual Practices in Civil Cases, Memoranda of Law are limited to 25 pages. While Defendants' memorandum is exactly 25 pages, it appears that they reduced the spacing between letters by half a point. This allows for an extra three lines per page, which, over the course of a 25-page brief, provides approximately three extra pages. Other courts in this district have sanctioned attorneys who use formatting tricks to submit overlong briefs. *See, e.g., CafeX Commc'ns, Inc. v. Amazon Web Servs., Inc.*, No. 17-01349, ECF No. 43 (S.D.N.Y. Mar. 30, 2017).

[3] Defendants ask that this Court dismiss under Rule 12(b)(1), 12(b)(6), "or both." (Dkt. 54 at 25.) But of course, this Court could not dismiss under both sections; if it finds that Plaintiffs lack Article III standing and dismisses under Rule 12(b)(1), this Court would have no jurisdiction to dismiss under Rule 12(b)(6). *See Carter v. HealthPort Techs., LLC*, 822 F.3d 47, 54-55 (2d Cir. 2016) ("[W]here a complaint is dismissed for lack of Article III standing … [s]uch a dismissal is one for lack of subject matter jurisdiction, and without jurisdiction, the district court lacks the power to adjudicate the merits of the case.") (internal citations omitted).

With respect to the Rule 12(b)(6) portion of the motion, Defendants make four arguments: (1) that Plaintiffs fail to allege an "interception" under the Wiretap Act, (2) that Plaintiffs consented to Defendants' conduct, (3) that Defendants were parties to the intercepted emails, and (4) that Plaintiffs fail to state a claim under any state law. Each of these arguments fails: Defendants' "interception" argument is premature and should not be decided until after discovery; Plaintiffs did not consent to anything beyond Defendants' cleaning up their email inboxes; Defendants were not parties to the emails they intercepted between Plaintiffs and third parties; and Plaintiffs state claims under New York law for unjust enrichment and breach of fiduciary duty.

I. PLAINTIFFS HAVE ARTICLE III STANDING.

Defendants argue that Plaintiffs lack Article III standing because they fail to allege an "injury in fact," one of the three elements comprising the "irreducible constitutional minimum" of standing. *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). That is wrong. Defendants' unauthorized accessing and selling of Plaintiffs' emails was an invasion of Plaintiffs' privacy that easily satisfies the "injury in fact" requirement.[4]

"To establish injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id*. at 1548 (internal

[4] Defendants rightly do not argue that the other two elements of standing, traceability and redressability, are lacking here. The invasion of Plaintiffs' privacy is clearly "traceable to the challenged conduct of [Defendants]," and would be "redressed by a favorable judicial decision." *Spokeo*, 136 S. Ct. at 1547.

quotations omitted). The Second Circuit has repeatedly—even after *Spokeo*—referred to this requirement as "a low threshold." *John v. Whole Foods Mkt. Grp.*, 858 F.3d 732, 736 (2d Cir. 2017) (internal quotations omitted).

The particularity prong can be dispensed with quickly. "For an injury to be particularized, it must affect the plaintiff in a personal and individual way." *Spokeo*. 136 S. Ct. at 1548. (internal quotations omitted). Here, Mr. Cooper alleges that Defendants accessed and sold *his* emails, and Ms. Parikh alleges that Defendants accessed and sold *her* emails. Plaintiffs are not asserting some undifferentiated harm to the public or injuries to other people; Defendants' alleged conduct personally affects each of them. And while Defendants assert that Ms. Parikh merely alleges that her Lyft receipts *may* have been sold to Uber, and that Mr. Cooper doesn't even allege that he was a Lyft user (dkt. 54 at 9), Defendants' sale of UnrollMe users' Lyft receipts to Uber was simply "one instance" of Defendants' access and sale of its users' emails (Compl. ¶ 28.) The Complaint is not limited to those emails, and it alleges that Defendants access and sell all sorts of emails and information from all UnrollMe users—including Ms. Parikh and Mr. Cooper. (*See, e.g.,* Compl. ¶¶ 3, 16-19, 27, 38, 47.)

Similarly, Plaintiffs' injuries are not conjectural or hypothetical. Defendants' argument on this point misunderstands the alleged injury. In Defendants' view, Plaintiffs' alleged injury is a "remote future harm" like identity theft or the misuse of their personal information by a third party. (*See* dkt. 54 at 9-11.) But while those may be *additional* harms that Plaintiffs might suffer, they are not the injuries

alleged here. Rather, Plaintiffs' injury is the invasion of their privacy resulting from Defendants' unauthorized access and sale of their emails. That conduct has already occurred and those injuries have already been sustained. In short, Plaintiffs' injury is "actual." *Spokeo*, 136 S. Ct. at 1548. As the Ninth Circuit explained in its decision on remand in *Spokeo*:

> [Defendant's] reliance on *Clapper* [*v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2016)] is misplaced. In *Clapper*, the plaintiffs sought to establish standing on the basis of harm they would supposedly suffer from *threatened conduct* that had not happened yet but which they believed was reasonably likely to occur…. Here, by contrast, both the challenged conduct and the attendant injury have already occurred…. It is of no consequence how likely [plaintiff] is to suffer *additional* concrete harm as well.

Robins v. Spokeo, Inc., 867 F.3d 1108, 1118 (9th Cir. 2017).

Finally, Plaintiffs' alleged injuries are concrete. As the Supreme Court held in *Spokeo*, "'[c]oncrete' is not … synonymous with 'tangible,'" and, thus, "intangible injuries can nevertheless be concrete." 136 S. Ct. at 1549. To determine whether an intangible harm constitutes a concrete injury in fact, courts look to both history and the judgment of Congress. *Id*. As to the former, "it is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts." *Id*. Plaintiffs' alleged intangible harm here—Defendants' invasion of their privacy—is just such a harm. *See Mount v. PulsePoint, Inc.*, No. 13-6592, 2016 WL 5080131, at *4 (S.D.N.Y. Aug. 17, 2016) ("Invasion of privacy is an intangible harm recognized by the common law.") (internal quotations and alteration omitted), *aff'd*, 684 Fed. Appx. 32 (2d. Cir. 2017); *Matera v. Google, Inc.*, No. 15-04062, 2016 WL 5339806, at

*10 (N.D. Cal. Sept. 23, 2016) ("Invasion of privacy has been recognized as a tort under common law for over a century."); *Rackemann v. LISNR, Inc.*, No. 17-00624, 2017 WL 4340349, at *4 (S.D. Ind. Sept. 29, 2017) (same). And as to Congressional judgment, by enacting the Wiretap Act and the Stored Communications Act, Congress has identified the privacy harms alleged here as concrete. *See Spokeo*, 136 S. Ct. at 1549 ("[B]ecause Congress is well positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important."); *Rackemann*, 2017 WL 4340349 at *5 ("[T]he Wiretap Act was passed to protect against the invasion of privacy, and particularly privacy with regard to electronic communications."); *Theofel v. Farey-Jones*, 359 F.3d 1066, 1072 (9th Cir. 2004) ("The [Stored Communications] Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage.").

Defendants argue that their invasion of Plaintiffs' privacy was not concrete because it was "at most … a 'bare procedural' violation." (Dkt. 54 at 14.) While the Court in *Spokeo* stated that a plaintiff "cannot satisfy the demands of Article III by alleging a bare procedural violation," 136 S. Ct. at 1550, "[t]his statement is inapplicable to the allegations at hand, because [Plaintiffs here] ha[ve] not alleged a procedural violation." *Church v. Accretive Health, Inc.*, 654 Fed. App'x 990, 995 n.2 (11th Cir. 2016). The statutes and common law on which Plaintiffs rely do not establish procedural rights, they provide Plaintiffs with substantive privacy protections. Defendants' unauthorized accessing and sale of their emails was thus a

substantive—not a bare procedural—violation. *See Boelter v. Hearst Commc'ns, Inc.*, No. 15-03934, 2017 WL 3994934, at *8 (S.D.N.Y. Sept. 7, 2017) ("Plaintiff's alleged injury is not a 'bare procedural violation,' but a substantive violation that strikes at the long-recognized right to privacy."); *Matera*, 2016 WL 5339806 at *13 ("Plaintiff alleges not a 'bare procedural violation.' Instead, Plaintiff alleges that [defendant] unlawfully intercepted, scanned, and analyzed Plaintiff's communications in violation of the Wiretap Act."); *Rackemann*, 2017 WL 4340349 at *3 ("The Court agrees that [plaintiff] has sufficiently identified as an injury the violation of his *substantive* interest in the privacy of his communications.") (emphasis added).

This is why Defendants' reliance on *Vigil v. Take-Two Software, Inc.*, 235 F. Supp. 3d 499 (S.D.N.Y. 2017) is unavailing. In that case, plaintiffs did not allege that the defendant had disseminated or misused plaintiffs' private information, only that it had failed to comply with certain statutory procedures required under state law when collecting that information. *Id.* at 502, 506-07. Thus, plaintiffs in that case alleged only "procedural violations." *Id.* at 510, 511, 514-15. According to the court in *Vigil*, the allegations "[could not] be construed to have established a claim based on any theory of invasion of privacy." *Id.* at 518 n.10 (distinguishing *Matera*). Here, in contrast, Plaintiffs are not alleging that Defendants failed to comply with mere procedural requirements, but that Defendants' invaded their substantive rights to privacy. Not surprisingly, courts have repeatedly found that invasions of privacy satisfy Article III's concreteness requirement. *See, e.g., Mejia v. Time Warner Cable Inc.*, No. 15-06445, 2017 WL 3278926, at *7 (S.D.N.Y. Aug. 1, 2017)

(holding that allegation of "precisely the sort of injury" that a law was designed to target—including invasion of privacy—supported Article III standing); *Mount v. PulsePoint, Inc.*, 684 Fed. App'x 32, 34 (2d Cir. 2017) (holding that "loss of privacy" was a concrete injury); *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016) (holding that "unauthorized disclosures of information that … ought to remain private" was an Article III injury in fact).

Simply put, Plaintiffs have Article III standing.

II. DEFENDANTS' 12(b)(6) MOTION SHOULD BE DENIED.

In addition to rejecting Defendants' standing argument, this Court should also deny the 12(b)(6) portion of their motion to dismiss. As noted above, Defendants make four arguments pursuant to Rule 12(b)(6): (1) that Plaintiffs fail to allege an "interception" under the Wiretap Act, (2) that Plaintiffs consented to Defendants' conduct, (3) that Defendants were parties to the intercepted emails, and (4) that Plaintiffs fail to state a claim under any state law. As explained more fully below, none of these arguments warrants dismissal.

A. Defendants' "Interception" Argument is Premature and Should Not Be Decided Until After Discovery.

The Wiretap Act bars any person from "intentionally intercept[ing] … any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). Defendants argue that Plaintiffs' Wiretap Act claim should be dismissed because the Complaint fails to allege an "interception" under the act. (Dkt. 54 at 20-22.) Specifically, Defendants argue that in order to constitute an interception under the Wiretap Act, an acquisition of a communication must be "contemporaneous with transmission" of

the communication (*id.*), and that the Complaint does not allege such contemporaneous acquisition.

No contemporaneous acquisition requirement appears in the Wiretap Act or the statutory definition of "interception," however. *Zaratzian v. Abadir*, No. 10-09049, 2014 WL 4467919, at *6 (S.D.N.Y. Sept. 2, 2014). Nevertheless, several circuit courts—though not the Second Circuit—have endorsed this "narrow" reading of the act. *See id.* (citing cases from the Third, Fifth, Ninth, and Eleventh Circuits). The Second Circuit has not addressed the question, and courts in this District do not appear to have reached any consensus. *See id*. (noting that at least two other courts in the district have adopted the narrow definition of intercept, but refusing itself to decide the question).

In any case, even assuming for the sake of argument—as the court in *Zaratzian* did—that the narrow "contemporaneous acquisition" definition of interception is correct, it would be premature to decide on this motion to dismiss whether Defendants "intercepted" Plaintiffs' emails. The Complaint alleges that Defendants accessed Plaintiffs' emails "between the time each such message was sent, on the one hand, and the time such message was read by the recipient." (Compl. ¶ 64.) The technical details regarding when and how Defendants actually accessed them will ultimately be revealed through discovery, but Defendants accessed Plaintiffs' emails either while they were being transmitted or while they were sitting in Plaintiffs' email inboxes (or perhaps at both times). If the former, Plaintiffs have a Wiretap Act claim; if the latter, Plaintiffs have a Stored

Communications Act claim. *Compare* 18 U.S.C. § 2511(1)(a) (barring interception of electronic communications) *with* 18 U.S.C. § 2701(a)(2) (barring obtaining communications in electronic storage). Either way, Plaintiffs' case will go forward on one or both claims. Certainly, if Plaintiffs hope to succeed on a Wiretap Act claim, they will ultimately need to establish that Defendants "intercepted" their emails. But as other courts have recognized, dismissing a Wiretap Act claim before Plaintiffs have had a chance to take discovery on the precise method and timing of Defendants' accessing their electronic communications is not appropriate. *See, e.g., Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 841 (N.D. Cal. 2014) ("While [defendant] may ultimately produce evidence showing that the messages were actually accessed while in storage, not during transmission, that issue is premature at this stage of the case, and would be better addressed as part of a motion for summary judgment with a more developed factual record."); *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1027-28 (N.D. Cal. 2014) (rejecting as premature defendant's 12(b)(6) argument that communications were accessed while in storage, not while in transit, and noting that court would consider the argument "at the summary judgment stage after discovery").

B. Plaintiffs Did Not Consent to Defendants' Conduct.

While Plaintiffs thus have either a Wiretap Act claim or a Stored Communications Act claim—depending on when and how their emails were accessed—Defendants argue that any such claims fail because Plaintiffs consented to or authorized Defendants' conduct. (Dkt. 54 at 17-18, 19-20.) But that simply is

not true. While Plaintiffs provided UnrollMe with access to their emails for the limited purpose of cleaning up their inboxes, they did not consent to Defendants' culling the content of their emails for personal consumption information and selling those emails to the highest bidder. And while Defendants point to fine print in UnrollMe's privacy policy, that fine print does not establish Plaintiffs' consent, and cannot be used by Defendants to escape liability here.

1. Providing access to clean up an email inbox is not consent to scrape emails for consumer data to sell.

Consent to access electronic communications "is not an all-or-nothing proposition." *In re Google Inc. Gmail Litig.*, No. 13-02430, 2013 WL 5423918, at *12 (N.D. Cal. Sept. 26, 2013); *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1046 (N.D. Cal. 2014). *See also Zaratzian*, 2014 WL 4467919, at *8 ("The parameters of consent may be circumscribed depending on the subtleties and permutations inherent in a particular set of facts."). Thus, consent to access communications for one purpose does not establish consent to access those same communications for other purposes. For example, in *Google Gmail*, while users of Gmail (an email system operated by Google) had consented to allow Google to "pre-screen, review, flag, filter, modify, refuse or remove any or all Content from" users' emails, the court there held that users had *not* consented to Google's interception of their emails "for the purpose of creating user profiles or providing targeted advertising." 2013 WL 5423918 at *13. Similarly, in *Backhaut*, the court held that while users of iMessage (a text message system operated by Apple) had consented to Apple's interception of their text messages "for the purpose of providing and improving the iMessage service" and

"[t]o facilitate delivery of [users'] iMessages," such consent did not allow Apple to intercept their messages for other purposes. 74 F. Supp. 3d at 1045-46. *See also Zaratzian*, 2014 WL 4467919 at *8-9 (finding a wife permitting her husband to establish and configure her email account and set password did not constitute wholesale consent to husband's reading of wife's personal emails); *Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 581-82 (11th Cir. 1983) (employee's consent to monitoring of business calls on employer's phone did not constitute consent to monitoring of personal calls on same phone); *Opperman v. Path, Inc.*, 84 F. Supp. 962, 992 (N.D. Cal. 2015) (finding it plausible that while app users were aware that app would scan their electronic address book for one purpose, they were not aware the app would use their address book information in other, unauthorized ways.).[5]

Here, based on Defendants' representations about UnrollMe, made before and during the signup process—including that UnrollMe is a way to "[c]lean up your inbox" and "[u]nsubscribe easily from whatever you don't want"—Plaintiffs and other UnrollMe users consented to Defendants' accessing their emails only for the limited purpose of decluttering their email inboxes and unsubscribing them from unwanted spam emails. (*See, e.g.,* Compl. ¶¶ 20, 29, 38, 45.) They certainly did not consent to Defendants' scanning the contents of all of their emails for valuable personal data to be sold for market research. Consent is determined under a

[5] While each of these cases (except *Opperman*) addresses consent only under the Wiretap Act, the Stored Communications Act likewise provides that consent can be for a limited purpose. 18 U.S.C. § 2701(a) (providing punishment for anyone who accesses communications in electronic storage without authorization *or who "exceeds an authorization"* to access such communications) (emphasis added).

"reasonable user standard," *Matera*, 2016 WL 5339806 at *17; *Backhaut*, 74 F. Supp. 3d at 1046, and it is ultimately a question of fact whether a defendant has exceeded the scope of consent, *Matera* 2016 WL 5339806 at *17; *Google Gmail*, 2013 WL 5423918 at *13 ("It is the task of the trier of fact to determine the scope of the consent and to decide whether and to what extent the interception exceeded that consent."). Plaintiffs' Complaint sufficiently alleges—especially when drawing all reasonable inferences in their favor, *see Beretta*, 524 F.3d at 392—that their consent was limited to cleaning their email inboxes and unsubscribing from spam, and that Defendants exceeded this consent.

2. The privacy policy's fine print does not establish consent to scrape emails for consumer data to sell.

In an attempt to establish that Plaintiffs consented to their conduct, Defendants point to some fine print in UnrollMe's privacy policy. (Dkt. 54 at 5-6.) This tactic is unavailing for at least four reasons.

First, the fine print only refers to actions in which Defendants "may"—not will—engage. (Compl. ¶ 31) ("We *may* collect [and] sell … information…," "We *may* disclose … and sell such messages and the data that we collect…," "We *may* collect and use your commercial transactional messages…") (emphasis added, quoting privacy policy). But knowledge of Defendants' capacity to access and sell information contained in emails is not consent for them to do so. *See Google Gmail*, 2013 WL 5423918 at *13 (holding that Google's terms of service, which stated that it "may" target advertisements based on the content of emails "demonstrates only that Google has the *capacity* to intercept communications, not that it will," and

thus, the terms were "defective in demonstrating consent"). Indeed, UnrollMe's CEO and Co-Founder acknowledged that they "weren't explicit enough" in obtaining consent. (Compl. ¶ 30.)

Second, even if the fine print establishes consent, it does not excuse interception of an electronic communication if done for an unlawful or tortious purpose. 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful … to intercept a[n]… electronic communication … where one of the parties to the communication has given prior consent to such interception *unless such communication is intercepted for the purpose of committing any criminal or tortious act*....") (emphasis added). Here, as explained in Part II.D below, Plaintiffs allege that Defendants accessed their emails for a tortious purpose: the exploitation of Plaintiffs' private and personal information for Defendants' own unjust enrichment and in breach of duties owed by them to Plaintiffs. Defendants' tortious purpose in accessing Plaintiffs' emails thus negates any consent Plaintiffs may have provided in the fine print of the privacy policy or otherwise.[6]

Third, enforcing the fine print terms of the privacy policy to establish consent would be unconscionable. Unconscionability "is a flexible doctrine with roots in equity" and its principle "is one of prevention of oppression and unfair surprise."

---

[6] While the Second Circuit has explained that this exception to consent requires that the communication be intercepted for the purpose of a tortious act that is independent of the act of the interception itself, *Caro v. Weintraub*, 618 F.3d 94, 96 (2d Cir. 2010), that is exactly what is occurring here. The alleged tortious act—the unauthorized sale of Plaintiffs' emails for Defendants' gain in breach of Plaintiffs' trust and confidence—is separate from the interception of those emails. *See id*. at 101 ("The language and history of the Wiretap Act indicate that Congress authored the [tortious or criminal purpose] exception to the one-party consent rule to prevent abuse stemming from *use* of the recording not the mere *act* of recording.").

Universal Leasing Servs., Inc. v. Flushing Hae Kwan Rest., 565 N.Y.S.2d 199, 200 (N.Y. App. Div. 1991). *See also In re Currency Conversion Fee Antitrust Litig.*, 361 F. Supp. 2d 237, 250 (S.D.N.Y. 2005) ("[T]he 'purpose of the unconscionability doctrine is to prevent unfair surprise and oppression.'") (quoting *David L. Threlkeld & Co. v. Metallgesellschaft Ltd. (London)*, 923 F.2d 245, 249 (2d Cir. 1991)). Here, Defendants advertised their product as simply a way to "[c]lean up your inbox" and "[u]nsubscribe easily from whatever [spam emails] you don't want." (Compl. ¶ 20 & Fig. 1.) It would be an oppressive, unfair surprise to users of UnrollMe to hold them to contrary fine print in an adhesion contract purporting to authorize Defendants' scraping and selling of private information from their emails. *See Spinelli v. Nat'l Football League*, No. 13-07398, 2016 WL 3926446, at *4-5 (S.D.N.Y. July 15, 2016) (finding unconscionability where plaintiffs were told one thing about a deal but literal terms of agreement said something else entirely). In *Spinelli*, plaintiff sports photographers agreed to license their photographs to Associated Press ("AP") in exchange for royalties collected by AP for all licenses that AP in turn granted to third parties. AP licensed the photographs for free to the National Football League ("NFL"), the single largest licenser of the photographs, and, because AP collected no royalties from the NFL for the free licenses, it passed no royalties on to the photographers. When the photographers sued to collect, AP argued that the literal terms of its agreement with the photographers only called for royalties to be paid to photographers when AP licensed the photographs to third parties through a "sale." The court held those terms unconscionable given that the photographers believed

the NFL would be a revenue-bearing licensee and the AP didn't tell the photographers it would instead give away licenses to the NFL for free. 2016 WL 3926446 at *5. *See also Spinelli v. Nat'l Football League*, 96 F. Supp. 3d 81, 91-98 (S.D.N.Y. 2015) (setting forth facts of the case).

Finally, even if Defendants can rely on the fine print to establish that Plaintiffs consented to the surreptitious gathering and sale of their emails, the fine print authorizes the disclosure only of "non-personal information—data in a form that does not permit direct association with any specific individual." (Compl. ¶ 31) (quoting privacy policy). In fact, the fine print expressly promises that "[i]f we do disclose such messages or data, all personal information contained in such messages will be removed prior to any such disclosure. (*Id*.) (quoting privacy policy). Here, Defendants did not sufficiently anonymize Plaintiffs' information before selling it to third parties. Not only can Plaintiffs be directly associated with their purportedly anonymous information through various data set analyses (*see* Compl. ¶ 34 & nn.10-11), *Defendants actually disclosed users' email addresses* (Compl. ¶ 35 & Fig. 8). Thus, Defendants didn't even comply with the fine print they argue authorizes their conduct.

For all these reasons—the privacy policy's defective language, Defendants' tortious purpose in accessing Plaintiffs' emails, the unconscionability of enforcing the privacy policy against Plaintiffs, and Defendants' failure to anonymize the disclosed emails—Defendants cannot rely on the fine print of the privacy policy to suggest that Plaintiffs' consented to their actions.

C. Defendants Were Not Parties to Plaintiffs' Emails.

Defendants also insist that they are not liable under the Wiretap Act because they were parties to Plaintiffs' emails. (Dkt. 54 at 15-17.) But Defendants were not parties to Plaintiffs' emails; the emails were communications between Plaintiffs and others. As one of the cases cited by Defendants states, "[t]autologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient." *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 143 (3d Cir. 2015). Here, Defendants were neither the sender nor the recipient of Plaintiffs' emails. (Compl. ¶¶ 66, 77.) Rather, as explained above, they—without authorization—intercepted or accessed emails between Plaintiffs and third parties.

Defendants argue that by authorizing UnrollMe to clean up their email inboxes, Plaintiffs made Defendants parties to their emails. (Dkt. 54 at 16.) But that defies common sense. Even if Plaintiffs had provided unlimited consent to Defendants' reading of their emails, that would not somehow transform Defendants into either a sender or recipient of—and thus a party to—those emails. If one of the Plaintiffs were to show a friend of theirs a letter they received in the mail, the friend would not become a party to the communication; the friend is just someone to whom the correspondence was shown.

Neither of the cases cited by Defendants supports their position. In both *Google Cookie Placement* and *In re Nickelodeon Consumer Privacy Litigation*, the Third Circuit simply held that "companies that place cookies on a computing device

are … parties to any communications that they acquired." *Nickelodeon*, 827 F.3d at 275 (citing *Google Cookie Placement*). Those panels so held because the cookies caused information to be sent directly from plaintiffs to the companies placing the cookies, and the communications at issue were thus directly between the plaintiffs and those companies. *See Google Cookie Placement*, 806 F.3d at 142 ("[P]laintiffs' browsers sent that information directly to the defendants' servers."). Here, in contrast, Defendants are not placing cookies on Plaintiffs' computers and the communications at issue are not between Plaintiffs and Defendants. Rather, Defendants are intercepting communications between Plaintiffs and third parties—communications to which Defendants simply are not a party.

D. Plaintiffs Allege State Common Law Claims for Unjust Enrichment and Breach of Fiduciary Duty.

Finally, Defendants argue that Plaintiffs "fail to state a claim under any state law." (Dkt. 54 at 22.) To the contrary, however, Plaintiffs state claims for unjust enrichment and breach of fiduciary duty under New York law.

1. Plaintiffs State a Claim for Unjust Enrichment.

Defendants argue that Plaintiffs cannot state a claim for unjust enrichment under New York law because Plaintiffs "do not allege that they performed any services for Unrollme or Slice." (Dkt. 54 at 25.) But the performance of services is not an element of unjust enrichment. "To state a claim for unjust enrichment in New York, a plaintiff must allege that (1) defendant was enriched; (2) the enrichment was at plaintiff's expense; and (3) the circumstances were such that equity and good conscience require defendants to make restitution." *Bancorp Servs.,*

LLC v. Am. Gen. Life. Ins. Co., No. 14-09687, 2016 WL 4916969, at *8 (S.D.N.Y. Feb. 11, 2016). Here, by misappropriating and subsequently selling Plaintiffs' private information about their consumption habits—information obtained by luring Plaintiffs to download software that promised simply to declutter their email inboxes—Defendants were enriched at Plaintiffs' expense in circumstances that equity and good conscience cannot countenance. Multiple courts have held that profiting off of someone else's information constitutes unjust enrichment. *See, e.g., id.* (holding that allegations "that [defendant] has been unjustly enriched because it retained [plaintiffs' confidential] information and used that information [to its benefit] … suffices to survive a motion to dismiss"); *Redf-Organic Recovery, LLC v. Rainbow Disposal Co.*, 985 N.Y.S.2d 10, 11 (N.Y. App. Div. 2014) ("The amended complaint also states a cause of action for unjust enrichment, since it alleges that plaintiff gave defendant confidential information and that defendant failed to compensate plaintiff for the value of the appropriated information."); *Exelis, Inc. v. SRC, Inc.*, No. 12-00858, 2013 WL 5464706, at *7-8 (N.D.N.Y. Sept. 30, 2013) (holding that allegations that defendants misappropriated information from plaintiffs and used it to their benefit stated claim for unjust enrichment).

Defendants also assert that Plaintiffs' unjust enrichment claim must be dismissed as duplicative of their other claims. (Dkt. 54 at 25.) But while Plaintiffs are certainly not entitled to duplicative *relief*, Fed. R. Civ. P. 8(a)(3) permits pleading duplicative theories—including unjust enrichment—in the alternative. *See, e.g., Burton v. iYogi, Inc.*, No. 13-06926, 2015 WL 4385665, at *11 (S.D.N.Y.

Mar. 16, 2015); *Chigrinskiy v. Panchenkova*, No. 14-04410, 2015 WL 1454646, at *18 (S.D.N.Y. Mar. 31, 2015); *In re Hellas Telecomms. (Luxembourg) II SCA*, 535 B.R. 543, 585 (Bankr. S.D.N.Y. 2015). In any event, Plaintiffs' unjust enrichment claim is not duplicative of their other claims. Plaintiffs' federal statutory claims are premised on Defendants' unlawful interception or accessing of Plaintiffs' emails, while their unjust enrichment claim is premised on Defendants' sale of those misappropriated emails. *See Global Packaging Servs., LLC v. Global Printing & Packaging*, 248 F. Supp. 3d 487, 496 (S.D.N.Y. 2017) ("To the extent Plaintiff seeks to assert a claim for unjust enrichment as an alternative theory of recovery and not duplicative of remaining claims, the motion to dismiss is denied.").

2. Plaintiffs State a Claim for Breach of Fiduciary Duty.

Plaintiffs also state a claim for breach of fiduciary duty under New York law. While the Complaint does not invoke the phrase "breach of fiduciary duty" or allege it in a separate count as a particular legal theory under which Plaintiffs are proceeding, so long as a complaint alleges facts to support the substantive plausibility of a claim, "it is unnecessary to set out a legal theory for the plaintiff's claim for relief." *Johnson v. City of Shelby, Miss.*, 135 S. Ct. 346, 347 (2014) (reversing dismissal for failure to invoke statute in complaint).

Plaintiffs' Complaint sufficiently alleges facts to support a breach of fiduciary duty claim under New York law. New York embraces a "flexible standard" of fiduciary duty:

> Broadly stated, a fiduciary relationship is one founded upon trust or confidence reposed by one person in the integrity and fidelity of

> another…. The rule embraces both technical fiduciary relations and those informal relations which exit whenever one man trusts in, and relies upon, another.

Am. Tissue, Inc. v. Donaldson, Lufkin & Jenrette Sec. Corp., 351 F. Supp. 2d 79, 102 (S.D.N.Y. 2004) (quoting *Penato v. George*, 383 N.Y.S.2d 900 (1976)). Here, Plaintiffs placed considerable trust in Defendants to access their emails only for the purpose of cleaning their inboxes and unsubscribing to spam emails. (Compl. ¶¶ 29, 37.) But Defendants went far beyond that, exploiting Plaintiffs' trust and confidence by surreptitiously collecting and selling their private data. (*Id.*) Whether termed fiduciary, or agency, or some other relationship of trust and confidence, Defendants' misuse of Plaintiffs' emails with which they had been entrusted was a tortious breach of duty. *See, e.g., U.S. v. Chestman*, 947 F.2d 551, 569 (2d Cir. 1991) ("Because the fiduciary obtains access to [another's] property to serve the ends of the fiduciary relationship, he becomes duty-bound not to appropriate the property for his own use. What has been said of an agent's duty of confidentiality applies with equal force…: an agent is subject to a duty to the principal not to use or to communicate information confidentially given him by the principal or acquired by him during the course of or on account of his agency.") (internal quotations omitted).

Furthermore, "[w]hether a fiduciary duty exists is necessarily fact-specific to the particular case." *Childers v. NY & Presbyterian Hosp.*, 36 F. Supp. 3d 292, 308 (S.D.N.Y. 2014) (internal quotations omitted). Thus, "[o]n a motion to dismiss, it is often impossible to say that plaintiff will be unable to prove the existence of a fiduciary relationship," and "a claim alleging the existence of a fiduciary duty

usually is not subject to dismissal under Rule 12(b)(6)." *Id*. (internal quotations omitted).

Thus, in addition to their federal claims, Plaintiffs sufficiently state claims under New York law.

CONCLUSION

Because Plaintiffs sufficiently allege a concrete injury in fact, the Complaint should not be dismissed under Fed. R. Civ. P. 12(b)(1). Likewise, because Plaintiffs state claims under both federal and state law, the Complaint should not be dismissed under Fed. R. Civ. P. 12(b)(6). Consequently, Defendants' motion to dismiss should be denied in its entirety.

Respectfully submitted,

JASON COOPER and **MEGHNA PARIKH**, individually and on behalf of all others similarly situated,

Dated: November 9, 2017

By: /s/ Rafey S. Balabanian
One of Plaintiffs' Attorneys

Rafey S. Balabanian (*Pro Hac Vice)*
rbalabanian@edelson.com
Lily E. Hough*
lhough@edelson.com
EDELSON PC
123 Townsend Street
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Noah M. Schubert (*Pro Hac Vice)*
nschubert@sjk.law
Kathryn Y. Schubert (*Pro Hac Vice)*
kschubert@sjk.law
SCHUBERT JONCKHEER & KOLBE LLP
Three Embarcadero Center, Suite 1650

San Francisco, California 94111
Tel: 415.788.4220
Fax: 415.788.0161

Attorneys for Plaintiffs and the Putative Classes

* *Pro Hac Vice Application Pending*

CERTIFICATE OF SERVICE

I, Rafey S. Balabanian, hereby certify that on November 9, 2017, I served the above and foregoing ***Plaintiffs' Response in Opposition to Defendants' Motion to Dismiss*** by causing true and accurate copies of such paper to be filed and transmitted to all counsel of record via the Court's CM/ECF electronic filing system.

/s/ Rafey S. Balabanian